AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

Claim 1 (currently amended): A data processing system, comprising:

a processor,

a non-volatile storage medium including configuration data that describes a configuration of the non-volatile storage medium,

a controller for managing data exchanges with the non-volatile storage medium and for invoking an uninterruptible software routine in response to first software attempting to access the configuration data;

the uninterruptible software routine having code for determining whether the first software is authorized to access ~~the configuration data~~ all portions of the non-volatile storage medium and for allowing or preventing any ~~access~~ read operation on the non-volatile storage medium according to the determination.

Claim 2 (original): The data processing system of claim 1, in which the first software is initialization software for initializing the data processing system.

Claim 3 (original): The data processing system of claim 1, wherein the configuration data comprises at least a portion of first data included in a data structure of the non-volatile storage medium.

Claim 4 (original): The data processing system of claim 3, wherein the data structure includes a Master Boot Record.

Claim 5 (original): The data processing system of claim 1, wherein the configuration data comprises executable code.

Claim 6 (original): The data processing system of claim 5, wherein the executable code includes Master Boot Code.

Claim 7 (previously presented): The data processing system of claim 1, wherein at least one of the configuration data and data associated with the first software are encrypted and the controller includes a decrypter of said at least one of the configuration data and the data associated with the first software.

Claim 8 (previously presented): The data processing system of claim 7, wherein the decrypter is arranged to, in response to a determination that the first software is authorized to access the configuration data, decrypt the configuration data, which has been encrypted, for deriving a decrypted version of the configuration data for supporting access to the nonvolatile storage medium.

Claim 9 (previously presented): The data processing system of claim 8, wherein the data associated with the first software comprises a decryption key for decrypting the encrypted configuration data.

Claim 10 (previously presented): The data processing system of claim 7, wherein the data associated with the first software includes a software signature of said first software, and the uninterruptible software routine has an embedded signature for comparison with the software signature to determine whether the first software is authorized to access the configuration data.

Claim 11 (previously presented): The data processing system of claim 7, wherein the decrypter is arranged to derive a decryption key in response to at least one of the data associated with the first software and the configuration data.

Claim 12 (previously presented): The data processing system of claim 1, wherein the controller is adapted to, in response to any attempt by the first software to access the configuration data, trap said attempt and send an SMI interrupt to the processor; and

the uninterruptible software routine includes a system management mode code executable only within a constrained or protected operating environment for disabling the controller's trap in response to a determination that the first software is authorized to access the configuration data.

Claim 13 (previously presented): The data processing system of claim 1 further comprising:

an operating system stored in the non-volatile storage medium; and

an operating system loader for loading the operating system for the data processing system; and

wherein the configuration data is arranged to provide access to the operating system loader to load the operating system from the non-volatile storage medium.

Claim 14 (previously presented): The data processing system of claim 1 wherein the first software is binary input output system (BIOS) code.

Claim 15 (currently amended): A system, comprising;

a processor,

a first non-volatile storage medium having first and second firmware, and

a second non-volatile storage medium for storing configuration data that describes a configuration of the second non-volatile storage medium;

the processor having a first mode of operation for executing the first firmware and a second mode of operation for executing the second firmware;

the processor being adapted to enter the second mode of operation and execute the second firmware in response to the first firmware, executing in the first mode of operation, at least attempting to access the configuration data;

wherein the second firmware, when executed by the processor, determines whether the first software is authorized to access ~~the configuration data~~ all portions of the second non-volatile storage medium, and allows or prevents any read operation on the second non-volatile storage medium according to the determination.

Claim 16 (currently amended): A method of controlling a data processing system, the system comprising a processor, first non-volatile storage storing first software and an uninterruptible software routine for executing within respective first and second modes of operation of the processor, and a second non-volatile storage medium storing configuration data that describes a configuration of the second non-volatile storage medium; the first software having associated identification data; the method comprising the steps of:

executing the uninterruptible software routine, in the second mode of operation of the processor, in response to the first software, executing within the first mode of operation of the processor, at least attempting to access the configuration data;

determining whether the first software is authorized to access ~~the configuration data~~ all portions of the second non-volatile storage medium; and

~~controlling access to the configuration data according to that determination~~ if the first software is not authorized, preventing any read operation on the second non-volatile storage medium.

Clam 17 (previously presented): The method of claim 16 wherein the uninterruptible software routine is executable only in the second mode of operation of the processor and includes accessing to authorization data that is accessible only in the second mode of operation of the processor, and the step of determining comprises the steps of:

comparing the identification data associated with the first software with the authorization data to determine whether or not they match; and

authorizing access or otherwise to the configuration data according to the comparison.

Claim 18 (original): The method of claim 17, wherein the comparing step comprises the steps of: subjecting at least the identification data to an algorithm to produce a processing result; comparing the processing result to the authorization data; and authorizing access or otherwise to the configuration data according to the comparison.

Claim 19 (previously presented): The method of claim 16, further comprising the step of ; subjecting at least the configuration data to a configuration data algorithm to produce second configuration data supporting access to the second nonvolatile storage medium.

Claim 20 (previously presented): The method of claim 19, wherein the subjecting step comprises decrypting the configuration data with a decryption key derived from the identification data to produce the second configuration data.

Claim 21 (original): A memory storing a computer program for causing the system of claim 16 to perform the method of claim 16.

Claim 22 (original): The computer system of claim 16 programmed to perform the method of claim 16.

Claim 23 (previously presented): The data processing system of claim 1, wherein the uninterruptible software routine has code for hanging the data processing system in response to a determination that the first software is not authorized to access the configuration data.

Claim 24 (previously presented): The data processing system of claim 1, wherein the controller is an I/O controller hub.

Claim 25 (previously presented): The method of claim 20, further comprising:

generating and sending an SMI interrupt to the processor in response to any attempt by the first software executing within the first mode of operation of the processor to access the configuration data;

upon receipt of the SMI interrupt, said processor switching from the first mode to the second mode of operation for executing the uninterruptible software routine; and

in response to the generation of the SMI interrupt, passing the identification data, as an interrupt parameter, to the uninterruptible software routine for comparison with the authorization data.